

Representaciones de Galois de curvas superelípticas sobre cuerpos locales

Angel Villanueva
Universidad Nacional de Cuyo

LATeN 2020
2 de Julio de 2020

Consideramos \mathcal{O} un anillo de valuación discreta, π un uniformizador local, K su cuerpo de fracciones y k su cuerpo residual de característica p ($K = \mathbb{Q}_p$).

Definition

Una *curva superelíptica* o n -cíclica es una curva obtenida por un cubrimiento cíclico de \mathbb{P}^1 . Están dadas por una ecuación de la forma

$$\mathcal{C} : y^n = f(x)$$

donde $f(x) \in \mathcal{O}[x]$, $\text{Disc}(f(x)) \neq 0$.

Queremos entender las representaciones de Galois de curvas sobre cuerpos globales.

Si \mathcal{C} es una curva superelíptica sobre un cuerpo de números, mirando las diferentes completaciones podemos calcular todas las representaciones de Weil-Deligne y en particular las L -series locales y el discriminante de la representación.

Hay muchos resultados en la literatura en este sentido. Intentamos relacionar resultados de [BW17] con la noción de cluster introducida por [DDMM18] para obtener información sobre algunos invariantes (e.g. los L -factores locales, la imagen de la inercia, el conductor, etc).

Modelo estable de \mathbb{P}^1

Sea \mathcal{R} el conjunto de raíces de $f(x)$. Consideramos las siguientes extensiones $K \subset K_1 = K[\mathcal{R}] \subset K_2 = K_1[\varepsilon_n, \sqrt[n]{\tilde{\pi}}]$, donde $\tilde{\pi}$ es un uniformizador local de K_1 .

Vamos a suponer $K = K_2$, (en particular $f(x)$ factoriza sobre K).

En [BW17] y [DDMM18] dan el siguiente algoritmo para construir el único modelo semiestable $(\mathcal{X}, \mathcal{D})$ de la curva marcada (\mathbb{P}_K^1, D) , donde

$$D = \sum_{r \in \mathcal{R}} [r] + \begin{cases} [\infty] & \text{si } n \nmid \deg(f(x)) \\ \emptyset & \text{si } n \mid \deg(f(x)) \end{cases}$$

El modelo semiestable de \mathcal{C} puede obtenerse del cubrimiento cíclico de grado n (es la normalización de \mathcal{X} en el cuerpo de funciones de \mathcal{C}).

Sea T el conjunto de triplas de distintos elementos de $\text{Supp}(D)$. Si $t = (a, b, c) \in T$ sea

$$\varphi_t(x) = \frac{(b-c)(x-a)}{(b-a)(x-c)}$$

la función coordenada que manda (a, b, c) a $(0, 1, \infty)$.

Se define una relación de equivalencia en T : dado $t_1, t_2 \in T$, $t_1 \sim t_2$ si $\varphi_{t_2} \circ \varphi_{t_1}^{-1}$ se extiende a un automorfismo de $\mathbb{P}_{\mathcal{O}}^1$ (i.e. corresponde a una matriz en $\text{PGL}_2(\mathcal{O})$).

El modelo semiestable \mathcal{X} consiste de una componente (línea proyectiva) por clase de equivalencia. Además, la fibra especial \overline{X} de \mathcal{X} es un árbol de rectas proyectivas.

Example

Sea \mathcal{C}/\mathbb{Q}_p la curva superelíptica dada por la ecuación

$$\mathcal{C}: y^6 = x(x-p^2)(x-p)(x-p-p^2)(x-2p)(x-2p-p^2)(x-1)(x-1-p)(x-1-2p)$$

Entonces $\mathcal{R} = \{0, p^2, p, p + p^2, 2p, 2p + p^2, 1, 1 + p, 1 + 2p\}$ y $S = \mathcal{R} \cup \{\infty\}$ (pues $6 \nmid \deg(f)$).

Decimos que una terna (a, b, c) está *ordenada* si $v(b - c) = v(a - c) \leq v(a - b)$. Y si (a, b, c) está ordenada, llamamos *radio* a $\mu = v(a - b)$.

Se tiene $(a, b, c) \sim (a', b', c')$ si y sólo si $v(a - b) = v(a' - b') = \mu$ y $a \equiv b \equiv a' \equiv b' \pmod{\pi^\mu}$.

Toda terna ordenada (a, b, c) es equivalente a (a, b, ∞) .

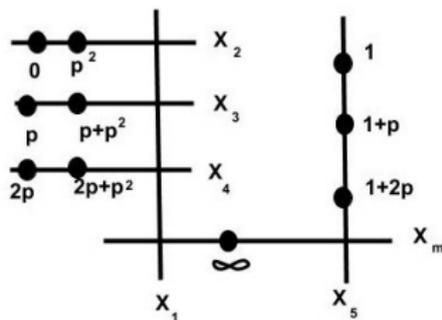
En nuestro caso, tenemos

$$t_0 = (0, 1, \infty), x_0 = x \quad t_3 = (p, p + p^2, \infty), x_3 = \frac{x - p}{p^2}$$

$$t_1 = (0, p, \infty), x_1 = \frac{x}{p} \quad t_4 = (2p, 2p + p^2, \infty), x_4 = \frac{x - 2p}{p^2}$$

$$t_2 = (0, p^2, \infty), x_2 = \frac{x}{p^2} \quad t_5 = (1, 1 + p, \infty), x_5 = \frac{x - 1}{p}$$

Entonces la fibra especial de \mathcal{X} se ve así



Clusters

Definition

Un *cluster* es un subconjunto de \mathcal{R} de la forma $\mathfrak{s} = D(z, d) \cap \mathcal{R}$ para algún disco $D(z, d) = \{x \in \overline{K} : v(x - z) \geq d\}$ donde $z \in \overline{K}$ y $d \in \mathbb{Q}$.

Un cluster *propio* es un cluster con más de un elemento.

Denotamos $\text{Cl}(\mathcal{R})$ al conjunto de clusters propios de \mathcal{R} .

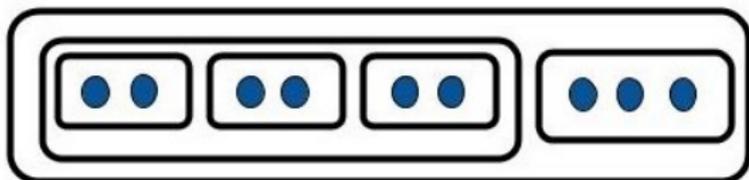
Definition

Si $\mathfrak{s}, \mathfrak{s}'$ son clusters con $\mathfrak{s}' \subset \mathfrak{s}$ un subcluster maximal, decimos que \mathfrak{s}' es un *hijo* de \mathfrak{s} y \mathfrak{s} el *padre* de \mathfrak{s}' .

A un cluster propio \mathfrak{s} asociamos su *profundidad*
 $\mu(\mathfrak{s}) = \min\{v(z - t) : z, t \in \mathfrak{s}\}.$

En nuestro ejemplo, tenemos

$$\mathcal{R} = \{0, p^2, p, p + p^2, 2p, 2p + p^2, 1, 1 + p, 1 + 2p\}.$$



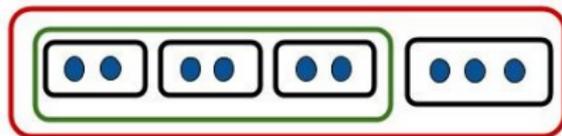
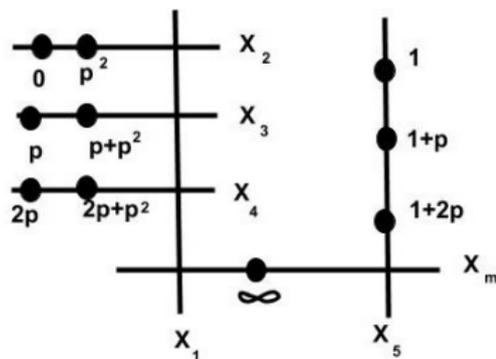
Los clusters son

$$s_m = \mathcal{R}, \quad s_1 = \{0, p^2, p, p + p^2, 2p, 2p + p^2\}, \quad s_2 = \{0, p^2\}$$
$$s_3 = \{p, p + p^2\}, \quad s_4 = \{2p, 2p + p^2\}, \quad s_5 = \{1, 1 + p, 1 + 2p\}.$$

Relación entre modelo minimal de \mathcal{X} y clusters

Sea (a, b, c) una tripla ordenada en T y sea $\mu = v(a - b)$ su invariante. Definimos $\Phi : T \rightarrow \text{Cl}(\mathcal{R})$ por

$$\Phi((a, b, c)) = D_\mu(a) \cap \mathcal{R}.$$



El modelo semiestable

La curva \mathcal{C} es un cubrimiento cíclico de \mathbb{P}^1 que viene de la función natural $\varphi : \mathcal{C} \rightarrow \mathbb{A}^1$, que manda (x, y) a x .

Sea \mathcal{Y} la normalización de \mathcal{X} en el cuerpo de funciones de Y_K , se tiene que \mathcal{Y} es el modelo semiestable de Y .

Sea π un uniformizador local de K . La fibra especial \overline{Y} de \mathcal{Y} es obtenida como sigue. Si $t \in T$ corresponde a una componente de la fibra especial de \overline{X} , $x_t := \varphi_t^*(x)$ el pullback de la coordenada estandar de X .

Si t corresponde a un cluster $\mathfrak{s} = D(r, d)$ (asumimos $r \in \mathcal{R}$) entonces las variables se relacionan por el cambio $x = \pi^d x_t + r$.

En nuestro ejemplo, $t_1 = (0, p, \infty)$, $x_1 = x/p$, entonces $x = px_1$.

Consideramos el polinomio $f(x_t)$ y c_t su valuación.

En nuestro ejemplo,

$$\mathcal{C}: y^6 = x(x-p^2)(x-p)(x-p-p^2)(x-2p)(x-2p-p^2)(x-1)(x-1-p)(x-1-2p)$$

$$\text{Luego } f(x) = f(px_1) =$$

$$p^6 x_1(x_1-p)(x_1-1)(x_1-1-p)(x_1-2)(x_1-2-p)(px_1-1)(px_1-1-p)(px_1-1-2p)$$

Tenemos que $c_1 = 6$.

Sea $f_t(x_t) = f(x_t)\pi^{-c_t}$, entonces obtenemos una curva con ecuación

$$\overline{\mathcal{Y}}_t : y_t^n = \overline{f}_t(x_t).$$

$$\mathcal{C}: y^6 = x(x-p^2)(x-p)(x-p-p^2)(x-2p)(x-2p-p^2)(x-1)(x-1-p)(x-1-2p)$$

Luego $f(x) = f(px_1) =$

$$p^6 x_1(x_1-p)(x_1-1)(x_1-1-p)(x_1-2)(x_1-2-p)(px_1-1)(px_1-1-p)(px_1-1-2p)$$

En nuestro ejemplo, $y_1 = y/p$. Tomamos reducción mod p .

$$\overline{\mathcal{Y}}_1 : y_1^6 = (-1)x_1^2(x_1-1)^2(x_1-2)^2 \Rightarrow \overline{\mathcal{Y}}_1^{(j)} : y_1^3 = (-1)^j i x_1(x_1-1)(x_1-2)$$

Observaciones: la curva \mathcal{Y}_t podría ser reducible, además, las componentes podrían no estar definidas sobre K_2 pero si sobre una extensión no ramificada de grado a lo más n .

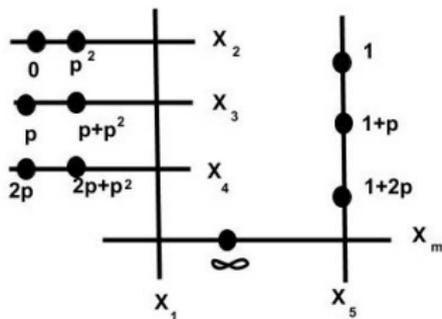
$$\overline{\mathcal{Y}}_1 : y_1^6 = (-1)x_1^2(x_1 - 1)^2(x_1 - 2)^2 \Rightarrow \overline{\mathcal{Y}}_1^{(j)} : y_1^3 = (-1)^j i x_1(x_1 - 1)(x_1 - 2)$$

Las otras componentes.

- ▶ $\overline{\mathcal{Y}}_m : y_m^6 = x_m^6(x_m - 1)^3 \Rightarrow \overline{\mathcal{Y}}_m^{(j)} : y_m^2 = \zeta_3^j x_m^2(x_m - 1)$
($y_m = y$)
- ▶ $\overline{\mathcal{Y}}_2 : y_2^6 = (-4)x_2(x_2 - 1)$ ($y_2 = y/p^{4/3}$).
- ▶ $\overline{\mathcal{Y}}_3 : y_3^6 = (-4)x_3(x_3 - 1)$ ($y_3 = y/p^{4/3}$).
- ▶ $\overline{\mathcal{Y}}_4 : y_4^6 = (-4)x_4(x_4 - 1)$ ($y_4 = y/p^{4/3}$).
- ▶ $\overline{\mathcal{Y}}_5 : y_5^6 = x_5(x_5 - 1)(x_5 - 2)$ ($y^5 = y/p^{1/2}$).

Si bien la curva $\overline{\mathcal{Y}}_m$ está definida sobre \mathbb{Z}_p , sus componentes están definidas sobre $\mathbb{Z}_p[\zeta_3]$ (el grupo de Galois actúa sobre las componentes).

Si $p \in \overline{X}_t$, el número de puntos de $x_t^{-1}(p)$ en \overline{Y}_t es igual a $r = \gcd(n, v(f_t))$.

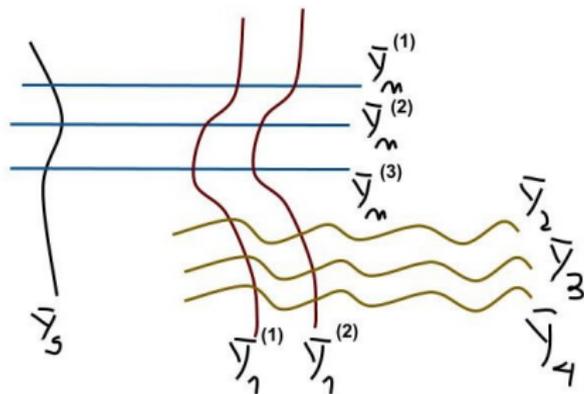


Los cortes corresponden en nuestras coordenadas, en identificar los puntos del infinito en la carta \mathfrak{s}' con el punto 0 en la carta asociada a \mathfrak{s} ($\mathfrak{s}' < \mathfrak{s}$).

Por ejemplo, $\bar{y}_m^{(j)} : y_m^2 = \zeta_3^j x_m^2 (x_m - 1)$. Si computamos la normalización en un entorno abierto de 0 (pero no de 1), la

ecuación \bar{Y}_m^j tiene ecuación
$$\begin{cases} z_m^2 = \zeta_3^j (x_m - 1) \\ z_m x_m = y_m \end{cases}$$

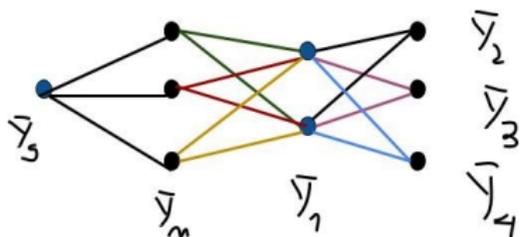
Entonces la preimagen de 0 en la j -th componente corresponde al punto $(0, 0, \pm\sqrt{-\zeta_3^j})$. En particular, corta a \bar{Y}_1 en 2 puntos. Luego, el gráfico de \bar{Y} es como sigue



Representación de Galois

Sea $\Upsilon = (V, E)$ el grafo dual de la fibra especial de \overline{Y} .

Es un grafo donde V son las componentes irreducibles de \overline{Y} y hay un lado uniendo vértices por cada punto de intersección entre las componentes.



Si consideramos el grupo de Picard $\text{Pic}^0(Y)$, contiene una parte abeliana y una tórica. El rango de la parte tórica es igual al rango de $H^1(\Upsilon, \mathbb{Z})$ y su representación de Galois consiste de bloques de Jordan 2×2 . Y la acción de $\text{Gal}(\overline{K}/K)$ sobre $Y(\overline{K})$ se extiende a una acción semilineal sobre los puntos geométricos de \overline{Y} .

En particular, tenemos un isomorfismo de G_K -representaciones

$$V_\ell(\text{Pic}^0(Y)) \simeq ((H^1(\Upsilon, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell) \otimes \text{Sp}_2) \oplus \bigoplus_{\tilde{Y} \in V} V_\ell(\text{Pic}^0(\tilde{Y})).$$

El rango de $H^1(\Upsilon, \mathbb{Z})$ es igual a $|E| - |V| + 1$.

En nuestro caso, $H^1(\Upsilon, \mathbb{Z}) = 7$.

Además, los géneros de las componentes son

$$g(\mathcal{Y}_m^{(j)}) = 0, \quad g(\mathcal{Y}_1^{(j)}) = 1 \quad (j = 1, 2), \quad g(\mathcal{Y}_2) = g(\mathcal{Y}_3) = g(\mathcal{Y}_4) = 2 \quad \text{y} \\ g(\mathcal{Y}_5) = 4.$$

Luego, la suma de los géneros con el rango de $H^1(\Upsilon, \mathbb{Z})$ es 19 como el género de \mathcal{C} .

En particular, la representación asociada a \mathcal{C} (asumiendo que K contiene $p^{1/3}$, ζ_3 , i) se descompone como suma directa de representaciones de dimensiones $1 + 1 + 2 + 2 + 2 + 4$ correspondiente a las curvas $\overline{\mathcal{Y}}_1^{(j)}$, $\overline{\mathcal{Y}}_2$, $\overline{\mathcal{Y}}_3$, $\overline{\mathcal{Y}}_4$, $\overline{\mathcal{Y}}_5$ y 7 bloques 2×2 donde la acción de Frobenius es trivial y un generador de la inercia actúa como $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Consideramos finalmente un ejemplo donde tomamos $K = \mathbb{Q}_5$ (sin raíces de la unidad ni del uniformizador).

Tomamos la curva \mathcal{C}/\mathbb{Q}_5 de género 4 dada por la ecuación

$$\mathcal{C} : y^3 = x^5 + 5 = \prod_{i=1}^5 (x - \alpha_i)$$

Tenemos que la extensión $\mathbb{Q}_p[x]/\langle x^5 + 5 \rangle$ es de orden 20. Sea π un uniformizador en la extensión. Se tiene que $v_\pi(\alpha_i) = \frac{v_\pi(5)}{5}$ pues $\prod_{i=1}^5 \alpha_i = 5$. Con lo cual $v_\pi(\alpha_i) = 4$.

Las raíces están distribuidas como el siguiente dibujo



La valuación en 5 del discriminante es 9. Como

$v_\pi(\text{disc}(f)) = v_\pi(\alpha_i - \alpha_j)^{20}$, se tiene que $v_\pi(\alpha_i - \alpha_j) = 9$.

Es decir, $\alpha_j - \alpha_k = \pi^9 t_{jk}$ con $t_{jk} \not\equiv 0 \pmod{\pi}$.

Se tiene $x_m = \frac{x - \alpha_1}{\alpha_2 - \alpha_1}$, $x = (\alpha_2 - \alpha_1)x_m + \alpha_1$, y

$$f(x_m) = \pi^{45} t_{21}^5 \prod_{i=1}^5 (x_m - \beta_i).$$

Luego, tenemos $y_m = \frac{y}{\pi^{15}}$, y $y_m^3 = t_{21}^5 \prod_{i=1}^5 (x_m - \beta_i)$.

El grupo de Galois de $\mathbb{Q}_5[x]/\langle x^5 + 5 \rangle$ es el subgrupo Γ de orden 20 de S_5 generado por $\Gamma = \langle (1\ 5\ 4\ 3\ 2), (2\ 3\ 5\ 4) \rangle$.

Este grupo tiene 4 representaciones de dimensión 1 (el 5-ciclo es un subgrupo normal y el cociente es cíclico de orden 4, son las reps. de dicho grupo) y una irreducible de dimensión 4.

Restringimos al grupo de inercia I_p .

Sea \tilde{I}_p el grupo de inercia de $\overline{\mathbb{Q}_p}/\mathbb{Q}_p[\mathcal{R}]$, $\rho_\ell(\tilde{I}_p) = 1$ porque la curva tiene buena reducción.

Si inducimos desde \tilde{I}_p hasta I_p , por la reciprocidad de Frobenius, la representación original aparece en esta representación (la representación regular, de dimensión 20).

En particular, es suma de irreducibles y de dimensión 4 (o suma de las de de dim. 1 o la de dim. 4).

En el primer caso, si vamos a la extensión de grado 4 normal de \mathbb{Q}_p , la imagen de la inercia sería trivial, o sea la curva tendría buena reducción en dicha extensión de grado 4, pero no puede ser pues el discriminante del polinomio tiene valuación 9, y al tener un y^3 , los cambios de variables involucran cambiar x por $\pi^3 x$ que cambia el discriminante en potencias de orden 60 pero $4 \cdot 9 = 36$ no es divisible por 60, en cambio arriba $20 \cdot 9 = 180$ si lo es.

Como el género de la curva es 4, la representación de Galois es de dimensión 8. Pero el anillo $\mathbb{Z}[\zeta_3]$ actúa en la rep. con lo cual la misma son dos copias de la rep. de dimensión 4. Si bien $\zeta_3 \notin \mathbb{Q}_5$ no importa pues la extensión $\mathbb{Z}_5[\zeta_3]$ es no ramificada (la imagen de inercia no cambia).

Entonces la matriz 4×4 asociada es la representación de dimensión 4 (la restricción a Γ de la representación estándar de S_5) de Γ que actúa en las raíces de $f(x)$.

Ya identificada la representación, calculamos el conductor de Artin, y así deducimos que tiene conductor 9.

- IRENE I. BOUW and STEFAN WEWERS. *Computing L-functions and semistable reduction of superelliptic curves*. *Glasg. Math. J.*, 59(1), 77–108, 2017.
- TIM DOKCHITSER, VLADIMIR DOKCHITSER, CELINE MAISTRET, and ADAM MORGAN. *Arithmetic of hyperelliptic curves over local fields*, arXiv preprint arXiv:1808.02936, 2018.
- ARIEL PACETTI and ANGEL VILLANUEVA. *Cyclic curves*. In progress.